

REMARKS

The specification has been amended. Claims 42, 47 - 51, 54 - 58, 61 - 66, 70 - 71, and 75 - 76 have been amended. No new matter has been introduced with these amendments, which are supported in the specification as originally filed. Claims 1 - 79 remain in the application.

L. Rejection Under 35 U.S.C. §102(a)

Paragraph 4 of the Office Action dated June 13, 2005 (hereinafter, "the Office Action") states that Claims 42 - 44, 51 - 52, 58 - 59, and 70 - 74 are rejected under 35 U.S.C. §102(a) as being anticipated by Request for Comments (hereinafter, "RFC") 2660. This rejection is respectfully traversed.

Applicants have amended their independent Claims 42, 51, 58, 65, 70, and 75 to more clearly specify limitations of their claimed invention. Applicants respectfully submit that these claims are patentable over RFC 2660, as will now be discussed.

The second limitation of independent Claims 42, 51, and 58, as amended herein, specifies "selecting, by said server application without using information from, or pre-arranged with, said client application, a message encoding scheme ..." (Claim 1, lines 8 - 9, emphasis added). The second limitation of independent Claims 65, 70, and 75 is similar.

By contrast, the cited Section 1.4.2 and Section 2.4.4 of RFC 2660 pertain to communications that take place when a client and server have shared or pre-arranged

information. See, for example, Section 1.4.2, which refers to use of “externally arranged keys” (Section 1.4.2, line 3) or “a prearranged session key” (Section 1.4.2, lines 6 - 7). The title of Section 2.4.4 is “Prearranged-Key-Info”, and states that this header “is intended to convey information about a key which has been arranged outside of the internal cryptographic format” (Section 2.4.4, lines 1 - 2, emphasis added). Lines 9 - 10 of the section further explain that an “inband” method for exchanging named keys indicates that the session key was “exchanged [between the parties] previously”, and lines 11 - 13 of this section explain that an “outband” method indicates that “the agents have external access” to key materials (which indicates a prior, or side-line, method with which information can be shared between the parties).

The cited Section 3.1 refers to Section 3.2 and 3.3. The cited Section 3.2.1, which comprises the overview of Section 3.2, discusses a negotiation header with which “Both parties are able to express their requirements and preferences regarding what cryptographic enhancements they will permit/require the other party to provide” (Section 3.2.1, lines 1 - 3, emphasis added). This Section 3.2.1 also provides an example whereby one party indicates that the other party can use either DES-CBC or RC2 for bulk encryption of messages. Suppose the client sends this example header. The client is then telling the server that either of two “message encoding schemes” (to use Applicants’ claim language) can be used by the server. This is distinct from Applicants’ claimed technique, where the server makes this decision (i.e., selects a message encoding scheme) “without using information from ... the client application” (Claim 42, lines 8 - 9, emphasis added; see also Claim 65, lines 7 - 8). Section 3.3 specifies, in its subsection 3.3.1, that the Encryption-Identity header “identifies a potential recipient for whom

the message ... could be encrypted" (Section 3.1.1, lines 1 - 2). In other words, the message sender (e.g., a client application) provides the message recipient (e.g., a server application) with information that can be used to select a message encoding scheme, in contrast to Applicants' claimed technique (where the server application does not use information from the client application to select the message encoding scheme).

RFC 2660 states, in Section 1.3.1, "Message Preparation", that creation of an S-HTTP message "can be thought of as a ... function with three inputs" (Section 1.3.1, lines 1 - 2), where the second input is the receiver's cryptographic preferences and keying material (Section 1.3.1, line 7) while the third input is the sender's cryptographic preferences and keying material (Section 1.3.1, line 10). This section continues by stating "In order to create an S-HTTP message, then, the sender integrates the sender's preferences with the receiver's preferences." (Section 1.3.1, lines 13 - 14, emphasis added). This is in contrast to Applicants' claimed technique, where the receiver (i.e., the server application) selects a message encoding scheme without using the cryptographic preferences and keying material of the sender (i.e., of the client application).

The final limitation of independent Claims 42, 51, and 58, as amended herein, specifies "piggy-backing security information onto a content response ... wherein said content response ... send[s] said encrypted security-sensitive content, wherein said piggy-backed security information enables said client application to determine said selected message encoding scheme, such that said client application can then decrypt said security-sensitive content" (Claim 42, lines 13 - 20,

emphasis added). The final limitation of independent Claims 65, 70, and 75 has similar language. Applicants find no analogous teachings in RFC 2660.

Furthermore, Applicants respectfully note that rejected Claims 72 - 74 and 77 - 79 are analogous to allowed Claims 67 - 69, and respectfully submit that these Claims 72 - 74 and 77 - 79 are therefore patentable as previously presented.

In view of the above, Applicants respectfully submit that RFC 2660 does not anticipate their independent Claims 42, 51, 58, 70, 72, 75, or 77. Dependent Claims 43 - 44, 52, 59, 71, 73 - 74, 76, and 78 - 79 are therefore deemed patentable over the reference as well, and the Examiner is respectfully requested to withdraw the §102 rejection of all claims.

II. Rejection Under 35 U.S.C. §103(a)

Paragraph 6 of the Office Action states that Claims 47 - 48, 50, 54 - 55, 57, 61 - 62, and 64 are rejected under 35 U.S.C. §103(a) as being unpatentable over RFC 2660 in view of the Examiner's Official Notice. This rejection is respectfully traversed.

Applicants have demonstrated, above, that independent Claims 42, 51, and 58 are patentable over RFC 2660. Thus, dependent Claims 47 - 48, 50, 54 - 55, 57, 61 - 62, and 64 are patentable over this art, whether taken singly or in combination with Official Notice. The Examiner is therefore respectfully requested to withdraw the §103 rejection.

III. Allowable Claims

Paragraph 7 of the Office Action states that Claims 45 - 46, 49, 53, 56, 60, and 63 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form to include all limitations of the base claim and any intervening claims. As demonstrated above, Applicants' independent Claims 42, 51, and 58 are deemed patentable over the references, and thus Applicants respectfully submit that dependent Claims 45 - 46, 49, 53, 56, 60, and 63 are allowable as currently presented.

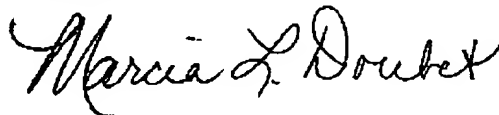
IV. Allowed Claims

Paragraph 8 of the Office Action states that Claims 1 - 41 and 65 - 69 are allowed. Applicants respectfully note that Claims 70 - 74 and 75 - 79 are analogous to allowed Claims 65 - 69, and incorporate all limitations from these allowed claims; however, Claims 70 - 74 and 75 - 79 have been rejected under 35 U.S.C. §102. As discussed above, Applicants respectfully submit that Claims 70 - 79 are allowable as currently presented.

V. Conclusion

Applicants respectfully request reconsideration of the pending rejected claims, withdrawal of all presently outstanding rejections, and allowance of all claims at an early date.

Respectfully submitted,



Marcia L. Doubet, Attorney for Applicants
Registration Nbr. 40,999

Customer Nbr. for Correspondence: 43168
Phone: 407-343-7586; Fax: 407-343-7587

Serial No. 09/415,645

-38-

Docket RSW9-99-084